

ABSTRACT

An encryption/decryption method and apparatus is disclosed which may comprise performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages; holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width; encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width; decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step; performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block. The method and apparatus may further comprise selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block and performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds. The method and apparatus may further comprise performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary; generating each round key by the expansion of a starting key of a second selected width. The second selected width may equal the first selected width; and, the encryption step may further include performing an affine transformation and the decryption step may further include performing an inverse

of the affine transformation.